

CLAIMS

What is Claimed is:

- 1 1. A system for controlling access to digital services comprising:
 - 2 (a) a control center configured to coordinate and provide digital services;
 - 3 (b) an uplink center configured to receive the digital services from the control center
 - 4 and transmit the digital services to a satellite;
 - 5 (c) the satellite configured to:
 - 6 (i) receive the digital services from the uplink center;
 - 7 (ii) process the digital services; and
 - 8 (iii) transmit the digital services and configuration information for accessing
 - 9 the digital services to a subscriber receiver station;
 - 10 (d) the subscriber receiver station configured to:
 - 11 (i) receive the digital services and configuration information from the
 - 12 satellite;
 - 13 (ii) control access to the digital services through an integrated
 - 14 receiver/decoder (IRD);
 - 15 (e) a conditional access module (CAM) communicatively coupled to the (IRD),
 - 16 wherein the CAM is configured to receive the configuration information, and wherein the
 - 17 configuration information has been transmitted asynchronously; and
 - 18 (f) a custom logic block within the CAM, wherein the custom logic block is
 - 19 configured to dynamically reconfigure a hardware state machine in the CAM based on the
 - 20 configuration information, wherein the hardware state machine comprises custom logic that is
 - 21 used to control access to the digital services.
 - 1 2. The system of claim 1 wherein the CAM comprises a smart card.
 - 1 3. The system of claim 1 wherein the configuration information is encrypted.

1 4. The system of claim 3 wherein the configuration information is encrypted
2 through a key exchange protocol.

1 5. The system of claim 4 wherein the key exchange protocol comprises a public
2 key algorithm.

1 6. The system of claim 3 wherein the configuration information is received in
2 uniquely encrypted, group encrypted packets.

1 7. The system of claim 3 wherein the custom logic block is further configured to:
2 decrypt the configuration information; and
3 store the configuration information in one or more protected registers.

1 8. The system of claim 1 wherein the custom logic block is further configured to
2 verify that the configuration information is authentic.

1 9. The system of claim 8 wherein the custom logic block is further configured to
2 retain the configuration information if the configuration information is authentic.

1 10. The system of claim 1 wherein the custom logic block is further configured to
2 receive a synchronous command to reconfigure the hardware state machine using the
3 configuration information.

1 11. The system of claim 1 wherein the hardware state machine is not directly
2 accessible to a system input/output module or system bus of the security component.

1 12. The system of claim 1 wherein the custom logic block comprises an
2 asynchronous dynamic pre-permutation module that employs a series of one or more
3 configurable multiplexors at the beginning of the hardware state machine.

1 13. The system of claim 1 wherein the custom logic block comprises an
2 asynchronous dynamic post-permutation module that employs a series of one or more
3 configurable multiplexors at the end of the hardware state machine.

1 14. The system of claim 1 wherein the custom logic block comprises a dedicated
2 hardware reconfiguration and input/output module that connects the hardware state machine to a
3 system bus of the CAM and controls access to logic of the hardware state machine.

1 15. A method for providing access to digital services comprising:
2 (a) receiving configuration information in a security component, wherein:
3 (1) the configuration information has been transmitted asynchronously; and
4 (2) the security component is configured to control access to the digital
5 services; and
6 (b) dynamically reconfiguring a hardware state machine in the security component
7 based on the configuration information, wherein the hardware state machine comprises custom
8 logic that is used to control access to the digital services.

1 16. The method of claim 15 wherein the security component comprises a smart
2 card.

1 17. The method of claim 15 wherein the configuration information is received
2 through a broadcast stream, Internet, callback, or other distribution channel.

1 18. The method of claim 15 wherein the configuration information is encrypted.

1 19. The method of claim 18 wherein the configuration information is encrypted
2 through a key exchange protocol.

1 20. The method of claim 19 wherein the key exchange protocol comprises a public
2 key algorithm.

10055660-022202

1 29. The method of claim 15 wherein a dedicated hardware reconfiguration and
2 input/output module connects the hardware state machine to a system bus of the security
3 component and controls access to logic of the hardware state machine.

- 1 30. A system for providing access to digital services comprising:
2 (a) a conditional access module (CAM) configured to receive configuration
3 information for accessing the digital services, wherein the configuration information has been
4 transmitted asynchronously; and
5 (b) a custom logic block configured to dynamically reconfigure a hardware state
6 machine in the CAM based on the configuration information, wherein the hardware state
7 machine comprises custom logic that is used to control access to the digital services.
- 1 31. The system of claim 30 wherein the CAM comprises a smart card.
- 1 32. The system of claim 30 wherein the configuration information is received through
2 a broadcast stream, Internet, callback, or other distribution channel.
- 1 33. The system of claim 30 wherein the configuration information is encrypted.
- 1 34. The system of claim 33 wherein the configuration information is encrypted
2 through a key exchange protocol.
- 1 35. The system of claim 34 wherein the key exchange protocol comprises a public
2 key algorithm.
- 1 36. The system of claim 33 wherein the configuration information is received in
2 uniquely encrypted, group encrypted packets.
- 1 37. The system of claim 33 wherein the custom logic block is further configured to:
2 decrypt the configuration information; and
3 store the configuration information in one or more protected registers.
- 1 38. The system of claim 30 wherein the custom logic block is further configured to
2 verify that the configuration information is authentic.

1 39. The system of claim 38 wherein the custom logic block is further configured to
2 retain the configuration information if the configuration information is authentic.

1 40. The system of claim 30 wherein the custom logic block is further configured to
2 receive a synchronous command to reconfigure the hardware state machine using the
3 configuration information.

1 41. The system of claim 30 wherein the hardware state machine is not directly
2 accessible to a system input/output module or system bus of the CAM.

1 42. The system of claim 30 wherein the custom logic block comprises an
2 asynchronous dynamic pre-permutation module that employs a series of one or more
3 configurable multiplexors at the beginning of the hardware state machine.

1 43. The system of claim 30 wherein the custom logic block comprises an
2 asynchronous dynamic post-permutation module that employs a series of one or more
3 configurable multiplexors at the end of the hardware state machine.

1 44. The system of claim 30 wherein the custom logic block comprises a dedicated
2 hardware reconfiguration and input/output module that connects the hardware state machine to a
3 system bus of the CAM and controls access to logic of the hardware state machine.

1 45. An article of manufacture for providing access to digital services comprising:
2 (a) means for receiving configuration information in a security component, wherein:
3 (1) the configuration information has been transmitted asynchronously; and
4 (2) the security component is configured to control access to the digital
5 services; and
6 (b) means for dynamically reconfiguring a hardware state machine in the security
7 component based on the configuration information, wherein the hardware state machine
8 comprises custom logic that is used to control access to the digital services.

10083860-00000000

1 46. The article of manufacture of claim 45 wherein the security component
2 comprises a smart card.

1 47. The article of manufacture of claim 45 wherein the configuration information is
2 received through a broadcast stream, Internet, callback, or other distribution channel.

1 48. The article of manufacture of claim 45 wherein the configuration information is
2 encrypted.

1 49. The article of manufacture of claim 48 wherein the configuration information is
2 encrypted through a key exchange protocol.

1 50. The article of manufacture of claim 49 wherein the key exchange protocol
2 comprises a public key algorithm.

1 51. The article of manufacture of claim 48 wherein the configuration information is
2 received in uniquely encrypted, group encrypted packets.

1 52. The article of manufacture of claim 48 further comprising:
2 means for decrypting the configuration information; and
3 means for storing the configuration information in one or more protected registers.

1 53. The article of manufacture of claim 45 further comprising means for verifying the
2 configuration information is authentic.

1 54. The article of manufacture of claim 53 further comprising means for retaining the
2 configuration information if the configuration information is authentic.

1 55. The article of manufacture of claim 45 further comprising means for receiving a
2 synchronous command to reconfigure the hardware state machine using the configuration
3 information.

59. The article of manufacture of claim 45 wherein a dedicated hardware
reconfiguration and input/output module connects the hardware state machine to a system bus of
the security component and controls access to logic of the hardware state machine.